REMARKS

By this amendment, claims 19-33 have been canceled without prejudice or disclaimer to the subject matter recited therein, and claim 34-45 have been added for consideration by the Examiner. In this regard, Applicants note that claims 34-36 are generally based on claims 19-21 respectively, claims 37-41 are generally based on claims 22-26 respectively, claims 42-44 are generally based on claims 27-29 respectively, and claim 45 is generally based on claim 32.

I. Claim Objections

Claims 19, 22, 26, 27, 30, 32 and 33 have been objected to due to minor informalities. By the present amendment, Applicants have submitted claims to remove the phrase "operable to" from the claims and to replace, for example, the phrase "operable to receive" with, for example, --for receiving--. Thus, Applicants respectfully request that the Examiner withdraw the objection.

II. Claim Rejections under 35 U.S.C. § 103(a)

Claims 19-33 have been rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,820,204 to DESAI et al. (hereinafter DESAI) in view of U.S. Patent No. 6,061,799 to ELDRIDGE et al. (hereinafter ELDRIDGE).

Applicants' claims 34-36 relate to a password recovery system for re-supplying a password. The system comprises a communication terminal device and a portable recording medium coupled to the communication terminal device. The communication terminal device includes a controller for receiving from an external communication terminal device a signed data set, based on an indication for recovering the password from a user of the communication terminal device. The external communication terminal device guarantees legitimacy of the user of the communication terminal device and generates the signed data set with a secret key. The controller outputs to the portable recording medium the received signed data sets. The portable recording medium includes a memory for storing the password and a public key corresponding to the secret key, and a controller for inputting from the communication terminal device the signed data set, and judging using the public key and the signed data set whether the signed data set is signed by the external communication terminal device. The controller of the portable recording medium recovers the same password as the password stored in the memory of the portable recording medium when it is judged that the signed data set is signed by the external communication terminal device, and outputs the recovered password to the communication terminal device. Claim 37-41 are drawn to the related communication terminal device. Claims 42-44 are drawn to the related portable recording medium. Claim 45 is drawn to a related method.

In direct contrast to the above-noted features, DESAI relates to a system for exchanging information, the system including a registered user 12, an information exchange system 10, and a third party 16 (Fig.1). As explained in DESAI, the information exchanging system 10 is responsible for storing profile data (e.g., telephone number, street address, and credit card number) of the registered user 12, with the profile data being kept private until the registered user 12 grants access thereto to one or more third parties 16 (see col. 8, lines 27-30, col. 8, lines 62-67 and col. 9, lines 4-10). In DESAI, it is explained that all of the data that is accessible to a registered user may be accessed upon the user logging onto the information exchange system and entering a password (see col. 15, lines 27-36).

However, DESAI fails to disclose or suggest at least a communication terminal device that receives from an external communication terminal device a signed data set, based on an indication for recovering the password from a user of the communication terminal device, the external communication terminal device generating the signed data set with a secret key, as well as a portable recording medium that judges using a public key corresponding to the secret key and the signed data set whether the signed data set is signed by the external communication terminal device, recovers the same password as the password stored in the memory of the portable recording medium when it is judged that the signed data set is signed by the external communication terminal device, and outputs the recovered password to the communication terminal device. Rather, in DESAI, when the registered user forgets his password, it is explicitly disclosed that the system has no way of recovering the lost password, and therefore, that a new password must be generated (see col. 15, lines 56-58). Thus, DESAI does not contain any disclosure regarding a system for recovering the same password as the password stored in the memory of the portable recording medium. As DESAI clearly discloses that there is no way to recover a lost password, Applicants respectfully submit that the information exchange system 10 of DESAI clearly does not correspond to the portable recording medium having the password recorded, as recited in, e.g., claim 34.

Thus, the pending claims are clearly distinguished over DESAI.

Therefore, it is respectfully submitted that the features recited in Applicants' pending claims are not disclosed or suggested by DESAI cited by the Examiner.

In setting forth the rejection, the Examiner relies on ELDRIDGE regarding that which the Examiner admits is lacking in DESAI. ELDRIDGE relates to a portable medium containing client process identification information. A computer system requires authentication prior to access to the client process identification information stored in the portable medium. The portable medium includes data identifying the client process and a plurality of data sets, each being associated with a password. One of the passwords is designated as current. The computer system determines whether any of the data associated with passwords matches authentication data previously stored in the computer system and associated with the client process. ELDRIDGE also teaches that an identification file 300 comprises a secret parameter 302 (see col. 4, lines 61-67 and col. 5, lines 1-14). One type of encryption key suitable for use secret parameter 302 is a RSA private encryption key, adhering to the RSA encryption standard (co1. 5, lines 15-24).

However, ELDRIDGE fails to disclose or suggest at least a communication terminal device that receives from an external communication terminal device a signed data set, based on an indication for recovering the password from a user of the communication terminal device, the external communication terminal device generating the signed data set with a secret key, as well as a portable recording medium that judges using a public key corresponding to the secret key and the signed data set whether the signed data set is signed by the external communication terminal device, recovers the same password as the password stored in the memory of the portable recording medium when it is judged that the signed data set is signed by the external communication terminal device, and outputs the recovered password to the communication terminal device. In this regard, it is noted that ELDRIDGE does not contain any disclosure regarding how to recover the password when a user forgets his password. Thus, because ELDRIDGE fails to disclose any way to recover a lost password, Applicants respectfully submit that the portable medium of ELDRIDGE clearly does not correspond to the portable recording medium having the password recorded, as recited in, e.g., claim 34.

Therefore, the pending claims are clearly distinguished over ELDRIDGE. Accordingly, it is respectfully submitted that the features recited in Applicants' pending claims are not disclosed or suggested by DESAI or ELDRIDGE cited by the Examiner.

Further, Applicants submit that even if one attempted to combine the teaching of DESAI with ELDRIDGE in the matter suggested by the Examiner, one would fail to arrive at the presently claimed invention, as such a combination would lack, at least, a communication terminal device that receives from an external communication terminal device a signed data set, based on an indication for recovering the password from user of the communication terminal device, the external communication terminal device generating the signed data set with a secret key, as well as a portable recording medium that judges using a public key corresponding to the secret key and the signed data set whether the signed data set is signed by the external communication terminal device, recovers the same password as the password stored in the memory of the portable recording medium when it is judged that the signed data set is signed by the external communication terminal device, and outputs the recovered password to the communication terminal device.

In view of the foregoing, Applicants submit that the suggested combination of DESAI with ELDRIDGE does not render the presently claimed invention obvious, and thus, respectfully request that the U.S.C. § 103(a) rejection be withdrawn.

Accordingly, Applicants respectfully request reconsideration and withdrawal of the outstanding rejection and an indication of the allowability of all the claims pending in the present application.

III. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may best be resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Motoji OHMORI et al.

By: /Kenneth W. Fields/
Digitally signed by /Kenneth W. Fields/
DN: cn=/Kenneth W. Fields/, o, ou,
email=kfields@wenderoth.com, c=US
Date: 2008.04.22 16:50:29 -04'00'

Kenneth W. Fields
Registration No. 52,430
Attorney for Applicants

KWF/mjw
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
April 22, 2008